

CLAIMS

Sub B1

1. System for processing an information signal, comprising a system (1) for scrambling the information signal and at least one system (2) for descrambling the scrambled information signal, said scrambling system comprising means (3,6) for analysing the entropy distribution of the information signal, means (5,6,7,9) for scrambling the information signal in dependence on the entropy distribution of the information signal to provide a scrambled information signal having an entropy distribution corresponding with the entropy distribution of the information signal and means (11) for compressing the scrambled information signal, said descrambling system (2) comprising means (14) for decompressing the compressed scrambled information signal, and means (16,19,21,22,24) for descrambling the scrambled information signal to provide the information signal.

2. System according to claim 1, wherein said scrambling means (5,6,7,9) comprises means (5,6,7) for generating a scrambling signal having an entropy distribution corresponding with the entropy distribution of the information signal and means (9) for combining the scrambling and information signals to obtain the scrambled information signal, wherein said descrambling means (16,19,21,22,24) comprises means (19,21,22,24) for regenerating the scrambling signal as a descrambling signal and means (16) for combining the descrambling and scrambled information signals to obtain the information signal.

3. System according to claim 2, wherein said analysing means (3,6) provides scrambling control information and wherein said generating means (5,6,7) generates a noise signal and comprises means (7) for processing said noise signal as controlled by the scrambling control information to obtain the scrambling signal, wherein said scrambling control information is transferred to the descrambling system (2), wherein said regenerating means (19,21,22,24) generates a noise signal and comprises means (22,24) for processing said noise signal as controlled by the scrambling

control information to obtain the descrambling signal.

4. System according to claim 3, wherein the scrambling control information is transferred to the descrambling system as part of the information signal.

a 5 5. System according to claim 3 ~~or 4~~, wherein said generating and regenerating means (5,7;21,22,24) comprises a white noise generator (5,21) and filtering means (7,22) controlled by said scrambling control information to filter the white noise to obtain noise having an entropy distribution corresponding with the entropy distribution of the information signal.

B 10 6. System according to claim 3 ~~or 4~~, wherein said generating and regenerating means (5,7;21,22,24) comprises a narrow band noise signal generator and modulating means for modulating the narrow band noise signal controlled by said scrambling control information to obtain noise having an entropy distribution corresponding with the entropy distribution of the information signal.

a 15 7. System according to claim 5 ~~or 6~~, wherein the noise generator of the generating means (5,7) is a pseudo random noise generator (5) seeded by a key, wherein said regenerating means (21,22,24) comprises a corresponding pseudo random noise generator (21) which is seeded by the same key, wherein means (6) are provided to transfer the key from the scrambling system (1) to the descrambling system (2) in a secure manner.

20 8. System according to claim 7, wherein the scrambling system (1) comprises means (6) for periodically generating a new key.

a 30 9. System according to claim 7 ~~or 8~~, wherein said scrambling system (1) comprises means (6) for generating entitlement files, wherein said transfer means (6) transfers an entitlement file together with a key to the descrambling system (2).

o 35 10. System according to claim 7, ~~8 or 9~~, wherein the transfer means (6) insert the key or entitlement file into the information signal to transfer this file as part of the information signal, preferably together with the scram-

bling control information.

a 11. System according to ^{claim 3} ~~any one of the claim 3-10~~,
wherein said scrambling system (1) is adapted to insert an
impulse response measuring signal into the information sig-
5 nal, wherein the descrambling system (2) is adapted to de-
termine the impulse response of the system by comparing the
received impulse response measuring signal with the original
impulse response measuring signal, the descrambling system
comprising an adjustable equaliser (24) to process the re-
10 generated noise signal, wherein the equaliser is adjusted to
model the transfer function of the system.

B) 12. System (1) for scrambling an information sig-
nal, comprising means (3,6) for analysing the entropy dis-
tribution of the information signal, means (5,6,7,9) for
15 scrambling the information signal in dependence on the en-
tropy distribution of the information signal to provide a
scrambled information signal having an entropy distribution
corresponding with the entropy distribution of the informa-
tion signal.

20 13. System according to claim 12, wherein said ana-
lysing means (3,6) provides scrambling control information
and wherein said scrambling means (5,6,7,9) comprises gener-
ating means (5,6) generating a noise signal and means (7)
for processing said noise signal as controlled by the scram-
25 bling control information to obtain the scrambling signal,
wherein means (6) are provided to transfer the scrambling
control information to a descrambling system (2).

30 14. System (2) for descrambling a scrambled infor-
mation signal, comprising means (16,19,21,22,24) for de-
scrambling the scrambled information signal to provide the
information signal, wherein said descrambling means com-
prises means (19,21,22,24) for regenerating the scrambling
signal as a descrambling signal and means (16) for combining
35 the descrambling and scrambled information signals to obtain
the information signal.

15. System according to claim 14, wherein said re-
generating means (19,21,22,24) generates a noise signal and
comprises means (22,24) for processing said noise signal to

obtain the descrambling signal.

16. System according to claim 15, wherein said regenerating means (19,21,22,24) comprises a white noise generator (21) and filtering means (22) to obtain noise having an entropy distribution corresponding with the entropy distribution of the information signal.

17. System according to claim 15, wherein said regenerating means (19,21,22,24) comprises a narrow band noise signal generator and modulating means for modulating the narrow band noise signal to obtain noise having an entropy distribution corresponding with the entropy distribution of the information signal.

18. System according to claim 16 ~~or 17~~, wherein the noise generator (21) is a pseudo random noise generator seeded by a key received from the scrambling system (1).

19. System according to ^{claim 15} ~~any one of claims 15-18~~, comprising means (19) for controlling said means (22,24) for processing said noise signal, wherein said controlling means (19) receives the scrambling control information and said processing means (22,24) is controlled in accordance with said scrambling control information to provide the descrambling signal.

20. System according to ^{claim 14} ~~any one of claims 14-19~~, wherein the scrambled information signal is compressed and decompressed, wherein the regenerating means (19,21,22,24) comprises means (24) for equalising the descrambling signal to compensate for compressing and decompressing of the original scrambling signal contained in the scrambled information signal.

21. System according to claim 20, wherein the equalising means (24) is adjustable by said controlling means (19), said controlling means being adapted to measure the impulse response of the compressing and decompressing operations and to adjust the equalising means to provide a corresponding impulse response.

22. System according to ^{claim 14} ~~any one of claims 14-21~~, wherein at least a part of the regenerating means (19,21,22,24), in particular the noise signal generator

(21), is accommodated in a secure device (20), for example a smart card.

23. System according to claim 22, wherein the secure device (20) is adapted to add a watermark signal to the descrambling signal.

24. System according to claim 22 ~~or 23~~, wherein the secure device (20) is adapted to add a compression hindering signal to the descrambling signal.

25. System according to ^{claim 14} ~~any one of claims 14-24~~, wherein the scrambled information signal and the descrambling signal are digital signals, wherein means are provided for converting the scrambled signal and the descrambling signal into analogue signals, wherein the combining means (16) combine the analogue signals to obtain a clear analogue information signal.

26. System according to claim 12 for scrambling audio signals, comprising a first plurality of first narrow band filters (26), each filter having an input receiving the audio signal and an output signalling the audio signal strength in the corresponding bandwidth, a processor (6) receiving the output signals of the narrow band filters to analyse the entropy distribution of the audio signal, said processor providing the scrambling control information, a pseudo random signal generator (5) having an output, a second plurality of second narrow band filters (27) corresponding to the first plurality of first narrow band filters (26), each second filter having an input connected to the output of the random signal generator (5) and an enable and gain control input, said processor (6) being connected to the enable and gain control inputs of the second filters, wherein the output signals of the second filters are combined to obtain a noise signal having an entropy distribution corresponding with the entropy distribution of the audio signal, and wherein the noise signal is combined with the audio signal to obtain a scrambled audio signal.

27. System ~~according to any one of claims 19-25~~ for descrambling a scrambled audio signal provided by the scrambling system of claim 26, wherein said processing means

(22,24) comprises a third plurality of narrow band filters (29), each filter having an input receiving the noise signal, an input receiving enable and gain control signals provided by the controlling means (19) in accordance with the scrambling control information, and an output, wherein the outputs of the filters are combined to provide the descrambling signal.

28. System according to claim 12 for scrambling still images, wherein the image information is divided in blocks and each block is transformed to obtain a set of coefficients, wherein the analysing means (3,6) analyses the entropy distribution of the transformed image information and provides the scrambling control information, wherein the generating means (5,6,7) generates noise in a two dimensional space and wherein the processing means (7) provides a filtered noise signal as scrambling signal.

29. System according to claim 28 for scrambling video, wherein a reference frame is processed as a still image, wherein next frames are compressed by determining differences with a reference frame and transforming the differences, wherein the scrambling signal used in the reference frame is reused in the next frames and wherein preferably the transformed difference signals are scrambled with a suitably processed scrambling signal.

30. System according to any one of claims 14-25 for descrambling video compressed by the system of claim 29, wherein said controlling means (19) controls the means (21,22,24) for regenerating the scrambling signal to reuse the regenerated scrambling signal for descrambling video frames which have been compressed by compressing differences with a reference frame.

31. Application of a system according to ~~anyone of~~ claims 11-20 for distribution of information, for example audio and/or video signals, comprising a central server (32-35,38) including means (34) for providing a key and entitlement file, means (33) for providing scrambled compressed information, and means (32) to transfer scrambled compressed information and a corresponding key and entitlement file to

~~one or more receiving systems (31,36) adapted to request such a transfer, each of said receiving systems having a secure device (20) receiving the key and entitlement file and providing an output used in descrambling the received scram-~~

5 bled compressed information.

Bl

1. Introduction